

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>

DATE(S) ISSUED:

05/10/2016

SUBJECT:

A Vulnerability in Windows Shell Could Allow for Arbitrary Code Execution (MS16-057)

OVERVIEW:

This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow for remote code execution if an attacker successfully convinces a user to browse to a specially crafted website that accepts user-provided online content, or convinces a user to open specially crafted content. Successful exploitation could result in the attacker gaining the same user rights as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE

There are no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Windows 8.1
- Windows Server 2012 R2
- Windows RT 8.1
- Windows 10

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:

A vulnerability exists when Windows Shell improperly handles object in memory which could allow for arbitrary code execution.

Successful exploitation could result in the attacker gaining the same user rights as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Do not visit untrusted websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.
- Consider implementing file extension whitelists for allowed e-mail attachments.

REFERENCES:

Microsoft:

<https://technet.microsoft.com/en-us/library/security/ms16-057>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0179>

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>